LƯỢC ĐỒ CHỮ KÝ SỐ XÂY DỰNG TRÊN TÍNH KHÓ CỦA BÀI TOÁN LOGARIT RỜI RẠC KẾT HỢP KHAI CĂN TRÊN Z_p

Nguyễn Đức Thụy[1*], Lưu Hồng Dũng[2]

Tóm tắt: *Bài báo đề xuất xây dựng lược đồ chữ ký số dựa trên tính khó của bài toán logarit rời rạc kết hợp khai căn trên Zp . Bài toán logarit rời rạc kết hợp khai căn được đề xuất ở đây là một dạng bài toán khó mới thuộc lớp các bài toán chưa có cách giải về mặt toán học. Phương pháp xây dựng lược đồ chữ ký số dựa trên tính khó của bài toán logarit rời rạc kết hợp khai căn này cho phép nâng cao độ an toàn của thuật toán. Ngoài ra, phương pháp xây dựng lược đồ chữ ký ở đây có thể áp dụng để phát triển một lớp thuật toán chữ ký số mới phù hợp với các ứng dụng yêu cầu cao về độ an toàn trong thực tế.*

Từ khóa: Thuật toán chữ ký số; Lược đồ chữ ký số; Bài toán Logarit rời rạc; Bài toán khai căn.

1. ĐẶT VẤN ĐỀ

Chữ ký số hiện nay đã được ứng dụng rộng rãi trong các lĩnh vực như Chính phủ điện tử, Thương mại điện tử,… hay trong các hệ thống viễn thông và mạng máy tính. Tuy nhiên, việc nghiên cứu, phát triển các lược đồ chữ ký số mới cho mục đích thiết kế - chế tạo các sản phẩm, thiết bị an toàn và bảo mật thông tin trong nước vẫn luôn là vấn đề cần thiết được đặt ra. Trong [1] đã đề xuất một phương pháp xây dựng thuật toán chữ ký số dựa trên tính khó của việc giải bài toán logarit rời rạc trên Z_p [2]. Ưu điểm của phương pháp mới đề xuất là từ đó có thể triển khai một lớp thuật toán chữ ký số cho các ứng dụng khác nhau. Tuy nhiên, độ an toàn của các thuật toán chữ ký được xây dựng theo phương pháp này chỉ được đảm bảo bởi độ khó của việc giải bài toán logarit rời rạc – DLP (Discrete Logarithm Problem) trên Z_p. Do đó, nếu có một giải thuật thời gian đa thức cho bài toán này (DLP) thì tính an toàn của các thuật toán sẽ bị phá vỡ hoàn toàn. Nâng cao độ an toàn cho các thuật toán chữ ký số dựa trên tính khó của việc giải đồng thời 2 bài toán khó là một hướng tiếp cận đang nhận được nhiều sự quan tâm của các nhà nghiên cứu, trong [3-13] các tác giả đã đề xuất một số thuật toán chữ ký xây dựng trên đồng thời hai bài toán phân tích số và logarit rời rạc. Trong bài báo này, cũng với mục đích nâng cao độ an toàn cho các thuật toán chữ ký số, nhóm tác giả tiếp tục phát triển phương pháp đề xuất trong [1] trên cơ sở tính khó giải của một bài toán mới, ở đây được gọi là bài toán logarit rời rạc kết hợp khai căn trên Z_p, ký hiệu: DLRP (Discrete Logarithm combining Finding Root Problem). Đây là một dạng bài toán khó lần đầu được đề xuất và ứng dụng cho việc xây dựng thuật toán chữ ký số và có nhiều triển vọng cho phép xây dựng các thuật toán phù hợp với các ứng dụng thực tế đòi hỏi độ an toàn cao.

2. BÀI TOÁN KHÓ MỚI VÀ PHƯƠNG PHÁP XÂY DỰNG THUẬT TOÁN CHỮ KÝ SỐ

2.1. Bài toán logarit rời rạc kết hợp khai căn trên Z_p

Bài toán được đề xuất ở đây là một dạng bài toán khó mới và được gọi là Bài toán logarit rời rạc kết hợp khai căn trên trường Z_p, dạng thứ nhất của bài toán này có thể phát biểu như sau:

Cho 2 số nguyên tố p, q thỏa mãn điều kiện: q|(p-1), với mỗi số nguyên dương $y \in Z_p^*$, hãy tìm các số q, x_1 và x_2 thỏa mãn phương trình sau:

$$\left(x_1\right)^{(x_1)^{-1}.x_2 \bmod q} \bmod p = y$$

Dạng thứ hai của bài toán logarit rời rạc kết hợp khai căn có thể được phát biểu như sau:

Cho số nguyên tố p, với các số nguyên dương $a,b,c \in Z_p^*$, hãy tìm số x thỏa mãn phương trình sau:

$$(a)^{c.x \bmod p} \equiv (x)^b \bmod p$$

Trong toán học, bài toán trên thuộc lớp các bài toán chưa có cách giải, các giải thuật cho bài toán logarit rời rạc – DLP (Discrete Logarithm Problem) hay bài toán khai căn – FRP (Finding Root Problem) trên Z_p hiện tại là không áp dụng được với DLRP.

2.2. Xây dựng lược đồ chữ ký dựa trên tính khó của bài toán mới đề xuất

2.2.1. Thuật toán sinh khóa

Ở phương pháp xây dựng thuật toán chữ ký mới đề xuất, bài toán DLRP được sử dụng để hình thành cặp khóa bí mật và công khai của các đối tượng ký. Trong đó, p là tham số hệ thống (tham số miền) do nhà cung cấp dịch vụ tạo ra, ở đây p là số nguyên tố cần phải được chọn sao cho việc giải bài toán DLP là khó. Các tham số (x_1, x_2, q) là khóa bí mật và y là khóa công khai tương ứng của mỗi đối tượng ký trong hệ thống. Để tạo khóa x_1 mỗi thực thể ký cần tạo trước số nguyên tố q thỏa mãn: q|(p – 1) và một số $\alpha \in Z_p^*$. Khóa x_1 được tạo theo:

$$x_1 = \alpha^{\frac{p-1}{q}} \bmod p$$

Khóa x_2 là một giá trị được chọn ngẫu nhiên trong khoảng (1, q). Sau đó, khóa công khai được tạo ra từ (x_1, x_2, q) theo (1):

$$y = (x_1)^{(x_1)^{-1} \times x_2 \bmod q} \bmod p \quad (1)$$

Thuật toán sinh khóa có thể được mô tả lại như trên bảng 1 sau đây:

Bảng 1. *Thuật toán sinh tham số và khóa.*

Input: lp, lq – độ dài (tính theo bit) của các số nguyên tố p,q. Output: p,q, x_1, x_2, y.
[1]. generate p,q: len(p) = lp, len(q) = lq, q|(p-1) [2]. select α: $1 < \alpha < p$ [3]. $x_1 \leftarrow \alpha^{(p-1)/q} \bmod p$ [4]. if (x_1 = 1) then goto [2] [5]. select x_2: $1 < x_2 < q$ [6]. $y \leftarrow (x_1)^{(x_1)^{-1}.x_2 \bmod q} \bmod p$ [7]. return {p,q, x_1, x_2,y}

Chú thích:

- len(.) : Hàm tính độ dài (theo bit) của một số nguyên;
- p: Tham số hệ thống/tham số miền;
- q, x_1, x_2: Khóa bí mật;
- y: Khóa công khai của đối tượng ký.

2.2.2. Thuật toán ký

Giả sử (R,S) là chữ ký lên bản tin M, u là 1 giá trị trong khoảng (1,q) và R được tính từ u theo công thức:

$$R = \left(x_1\right)^u \bmod p \tag{2}$$

Và S được tính từ v theo công thức:

$$S = \left(x_1\right)^v \bmod p \tag{3}$$

Ở đây: v cũng là 1 giá trị trong khoảng (1,q).

Cũng giả thiết rằng, phương trình kiểm tra của lược đồ có dạng:

$$\left(S\right)^E \equiv \left(R\right)^y \times \left(y\right)^{R \times S \bmod p} \bmod p$$

Với:

$$E = H(M) \text{ và: } R \times S \bmod p = \left(x_1\right)^k \bmod p \tag{4}$$

Trong đó: H(.) là hàm băm và $k \in Z_q^*$.

Đặt:

$$\left(x_1\right)^k \bmod p = Z \tag{5}$$

Khi đó, có thể đưa phương trình kiểm tra về dạng:

$$\left(S\right)^E \equiv \left(R\right)^y \times \left(y\right)^Z \bmod p \tag{6}$$

Từ (1), (2), (3) và (6) ta có:

$$\left(x_1\right)^{v.E} \equiv \left(x_1\right)^{u.y} \times \left(x_1\right)^{\left(x_1\right)^{-1}.x_2.Z} \bmod p \tag{7}$$

Từ (7) suy ra:

$$v \times E \equiv \left(u \times y + \left(x_1\right)^{-1} \times x_2 \times Z\right) \bmod q$$

Nên:

$$v = E^{-1} \times \left(u \times y + \left(x_1\right)^{-1} \times x_2 \times Z\right) \bmod q \tag{8}$$

Mặt khác, từ (2), (3) và (4) ta có:

$$\left(v + u\right) \bmod q = k \tag{9}$$

Từ (8) và (9) ta có:

$$k = u + E^{-1} \times \left(u \times y + \left(x_1\right)^{-1} \times x_2 \times Z\right) \bmod q \tag{10}$$

Từ (10), suy ra:

$$u = \left(k - \left(x_1\right)^{-1} \times x_2 \times Z \times E^{-1}\right) \times \left(E^{-1} \times y + 1\right)^{-1} \bmod q \tag{11}$$

Từ (11) và (8), có thể tính thành phần thứ nhất của chữ ký theo (2):

$$R = \left(x_1\right)^u \bmod p$$

và thành phần thứ 2 theo (3):

$$S = \left(x_1\right)^v \bmod p$$

Từ đây, thuật toán ký được mô tả trên bảng 2 như sau:

Bảng 2. *Thuật toán ký.*

Input: p, q, x_1, x_2, y, M. Output: (R,S).
[1]. $E \leftarrow H(M)$ [2]. select k: $1 < k < q$ [3]. $Z \leftarrow (x_1)^k \bmod p$ [4]. $u \leftarrow \left(k - (x_1)^{-1} \times x_2 \times Z \times E^{-1}\right) \times \left(E^{-1} \times y + 1\right)^{-1} \bmod q$ [5]. $v \leftarrow E^{-1} \times \left(u \times y + (x_1)^{-1} \times x_2 \times Z\right) \bmod q$ [6]. $R \leftarrow (x_1)^u \bmod p$ [7]. $S \leftarrow (x_1)^v \bmod p$ [8]. return (R,S)

Chú thích:

- M: bản tin cần ký, với: $M \in \{0,1\}^{\infty}$;
- (R,S): chữ ký của U lên M.

2.2.3. Thuật toán kiểm tra chữ ký

Thuật toán kiểm tra của lược đồ được giả thiết là:

$$(S)^E \equiv (R)^y \times (y)^{R \times S \bmod p} \bmod p$$

Ở đây, E là giá trị đại diện của bản tin cần thẩm tra: $E = H(M)$. Nếu M và chữ ký (R,S) thỏa mãn đẳng thức trên thì chữ ký được coi là hợp lệ và bản tin sẽ được xác thực về nguồn gốc và tính toàn vẹn. Ngược lại, thì chữ ký bị coi là giả mạo và bản tin bị phủ nhận về nguồn gốc và tính toàn vẹn. Do đó, nếu vế trái của đẳng thức kiểm tra được tính theo:

$$A = (S)^E \bmod p \tag{12}$$

và vế phải được tính theo:

$$B = (R)^y \times (y_2)^{\overline{Z}} \bmod p \tag{13}$$

ở đây:

$$\overline{Z} = R \times S \bmod p \tag{14}$$

Thì điều kiện chữ ký hợp lệ là: A = B.

Khi đó, thuật toán kiểm tra của lược đồ mới đề xuất được mô tả trong bảng 3 như sau:

Bảng 3. *Thuật toán kiểm tra.*

Input: p, y, M, (R,S). Output: *true* / *false* .
[1]. $E \leftarrow H(M)$ [2]. $A \leftarrow (S)^E \bmod p$ [3]. $\overline{Z} \leftarrow R \times S \bmod p$ [4]. $B \leftarrow (R)^y \times (y)^{\overline{Z}} \bmod p$ [5]. if (A=B) then {return *true*} else {return *false*}

Chú thích:

- M, (R,S): bản tin, chữ ký cần thẩm tra;
- Nếu kết quả trả về là *true* thì tính toàn vẹn và nguồn gốc của M được khẳng định. Ngược lại, nếu kết quả là *false* thì M bị phủ nhận về nguồn gốc và tính toàn vẹn.

2.2.4. Tính đúng đắn của lược đồ mới đề xuất

Điều cần chứng minh ở đây là: Cho p, q là 2 số nguyên tố với:

$$q \mid (p-1),\ H:\{0,1\}^* \mapsto Z_n, \mid q \mid \leq \mid n \mid < \mid p \mid, 1<\alpha<p, x_1 = \alpha^{(p-1)/q} \bmod p, 1<x_2<q,$$

$$y = (x_1)^{(x_1)^{-1} \times x_2 \bmod q} \bmod p, E = H(M), 1<k<q, Z = (x_1)^k \bmod p,$$

$$u = \left(k - (x_1)^{-1} \times x_2 \times Z \times E^{-1}\right) \times \left(E^{-1} \times y + 1\right)^{-1} \bmod q,$$

$$v = E^{-1} \times \left(u \times y + (x_1)^{-1} \times x_2 \times Z\right) \bmod q,\ R = (x_1)^u \bmod p,\ S = (x_1)^v \bmod p.$$

Nếu: $\overline{Z} = R \times S \bmod p$, $A = (S)^E \bmod p$, $B = (R)^y \times (y)^{\overline{Z}} \bmod p$ thì: $A = B$.

Tính đúng đắn của lược đồ mới đề xuất được chứng minh như sau:

Từ (3), (8) và (12) ta có:

$$A = (S)^E \bmod p = (x_1)^{v.E} \bmod p = (x_1)^{(E)^{-1}.\left(u.y+(x_1)^{-1}.x_2.Z\right).E} \bmod p = (x_1)^{\left(u.y+(x_1)^{-1}.x_2.Z\right)} \bmod p \quad (15)$$

Với:

$$u = \left(k - (x_1)^{-1} \times x_2 \times Z \times E^{-1}\right) \times \left(E^{-1} \times y + 1\right)^{-1} \bmod q \text{ và : } Z = (x_1)^k \bmod p$$

Từ (2), (3), (5), (8), (11) và (14) ta lại có:

$$\begin{aligned} \overline{Z} &= R \times S \bmod p = (x_1)^u \times (x_1)^v \bmod p = (x_1)^{u+v} \bmod p \\ &= (x_1)^{u+u.(E)^{-1}.y+(E)^{-1}.(x_1)^{-1}.x_2.Z} \bmod p = (x_1)^{u.\left(E^{-1}.y+1\right)+(E)^{-1}.(x_1)^{-1}.x_2.Z} \bmod p \\ &= (x_1)^{\left(k-(x_1)^{-1}.x_2.(E)^{-1}.Z\right).\left((E)^{-1}.y+1\right)^{-1}.\left((E)^{-1}.y+1\right)+(E)^{-1}.(x_1)^{-1}.x_2.Z} \bmod p = (x_1)^k \bmod p = Z \end{aligned} \quad (16)$$

Thay (1), (2), (5) và (16) vào (13) ta được:

$$\begin{aligned} B &= (R)^y \times (y)^{\overline{Z}} \bmod p = (x_1)^{u.y} \times (x_1)^{(x_1)^{-1}.x_2.Z} \bmod p \\ &= (x_1)^{\left(u.y+(x_1)^{-1}.x_2.Z\right)} \bmod p \end{aligned} \quad (17)$$

Từ (15) và (17) suy ra điều cần chứng minh: A=B.

2.2.5. Mức độ an toàn của lược đồ mới đề xuất

Mức độ an toàn của lược đồ mới đề xuất có thể đánh giá qua khả năng chống lại một số dạng tấn công như:

- Tấn công khóa bí mật:

Ở lược đồ mới đề xuất, các tham số (x_1,x_2,q) cùng được sử dụng làm khóa bí mật để hình thành chữ ký. Vì thế, lược đồ chỉ bị phá vỡ nếu cả 3 tham số này cùng bị lộ, nói cách khác là kẻ tấn công phải giải được bài toán logarit rời rạc kết hợp khai căn trên Z_p. Do đó, mức độ an toàn của lược đồ mới đề xuất xét theo khả năng chống tấn công làm lộ khóa bí mật được đánh giá bằng mức độ khó của việc giải được DLRP. Cần chú ý, DLRP là một

dạng bài toán khó mới, mà ngay cả khi có các giải thuật thời gian đa thức cho FRP và DLP cũng không có nghĩa là sẽ giải được bài toán này.

- Tấn công giả mạo chữ ký:

Từ thuật toán kiểm tra (bảng 3) của lược đồ mới đề xuất cho thấy, một cặp (R,S) giả mạo sẽ được công nhận là chữ ký hợp lệ với một bản tin M nếu thỏa mãn điều kiện:

$$(S)^E \equiv (R)^y \times (y)^{R.S \bmod p} \bmod p \tag{18}$$

Từ (18), nếu chọn trước R rồi tính S thì khi đó, điều kiện (18) sẽ có dạng:

$$(S)^E \equiv (a)^{b.S \bmod p} \bmod p \tag{19}$$

Còn nếu chọn trước S rồi tính R thì khi đó, điều kiện (18) sẽ trở thành:

$$(R)^y \equiv (a)^{b.R \bmod p} \bmod p \tag{20}$$

Với *a* và *b* là hằng số, dễ thấy rằng, (19) và (20) chính là dạng thứ hai của bài toán logarit rời rạc kết hợp khai căn trên Z_p.

3. KẾT LUẬN

Bài báo đề xuất xây dựng lược đồ chữ ký số theo một phương pháp mới dựa trên tính khó giải của bài toán logarit rời rạc kết hợp khai căn trên Z_p. Mức độ an toàn của lược đồ xây dựng theo phương pháp này được đảm bảo bằng mức độ khó của việc giải bài toán trên. Ở đây, bài toán logarit rời rạc kết hợp khai căn trên Z_p là một dạng bài toán khó mới, lần đầu được đề xuất và ứng dụng trong việc xây dựng thuật toán chữ ký số. Từ phương pháp mới đề xuất có thể xây dựng một lớp thuật toán chữ ký số có độ an toàn cao cho các ứng dụng trong thực tế.

TÀI LIỆU THAM KHẢO

[1]. Nguyen Duc Thuy and Luu Hong Dung, *"A New Construction Method of Digital Signature Algorithms",* IJCSNS International Journal of Computer Science and Network Security. Vol. 16 No. 12 pp. 53-57, December 2016. ISSN: 1738 - 7906.

[2]. T. ElGamal (1985). *"A public key cryptosystem and a signature scheme based on discrete logarithms"*. IEEE Transactions on Information Theory. Vol. IT-31, No. 4. pp.469–472.

[3]. Q. X. WU, Y. X. Yang and Z. M. HU, *"New signature schemes based on discrete logarithms and factoring",* Journal of Beijing University of Posts and Telecommunications, vol. 24, pp. 61-65, January 2001.

[4]. Z. Y. Shen and X. Y. Yu, *"Digital signature scheme based on discrete logarithms and factoring",* Information Technology, vol. 28,pp. 21-22, June 2004.

[5]. Shimin Wei, *"Digital Signature Scheme Based on Two Hard Problems",* IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.12, December 2007.

[6]. Eddie Shahrie Ismail, Tahat N.M.F., Rokiah. R. Ahmad, *"A New Digital Signature Scheme Based on Factoring and Discrete Logarithms",* Journal of Mathematics and Statistics, 04/2008; 12(3). DOI: 10.3844/jmssp.2008.222.225 Source:DOAJ.

[7]. Qin Yanlin , Wu Xiaoping*,"New Digital Signature Scheme Based on both ECDLP and IFP",* Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on, 8-11 Aug. 2009, E-ISBN : 978-1-4244-4520-2, pp 348 - 351.

[8]. Swati Verma1, Birendra Kumar Sharma, *"A New Digital Signature Scheme Based on Two Hard Problems",* International Journal of Pure and Applied Sciences and Technology, ISSN 2229 – 6107, Int. J. Pure Appl. Sci. Technol., 5(2) (2011), pp. 55-59.

[9]. Sushila Vishnoi , Vishal Shrivastava, *"A new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem",* International Journal of Computer Trends and Technology, volume 3, Issue 4, 2012.

[10]. A.N. Berezin, N.A. Moldovyan, V.A. Shcherbacov, *"Cryptoschemes Based on Difficulty of Simultaneous Solving Two Different Difficult Problems",* Computer Science Journal of Moldova, vol.21, no.2(62), 2013.

[11]. Phạm Văn Hiệp, Nguyễn Hữu Mộng, Lưu Hồng Dũng, *"Một thuật toán chữ ký xây dựng dựa trên tính khó của việc giải đồng thời hai bài toán phân tích số và logarit rời rạc",* Tạp chí Khoa học và Công nghệ Đại học Đà Nẵng, số 7(128). 2018, ISSN: 1859 – 1531.

[12]. Phạm văn Hiệp, Lưu Hồng Dũng, *"Chữ ký số tập thể và mô hình ứng dụng",* Tạp chí Nghiên cứu KH và CN Quân sự, số Đặc san CNTT, 11 – 2018, ISSN: 1859 – 1043.

[13]. Nguyễn Vĩnh Thái, Lưu Hồng Dũng, *"Một lược đồ chữ ký xây dựng trên tính khó của việc giải đồng thời 2 bài toán phân tích số và logarit rời rạc trên Zp",* Tạp chí Nghiên cứu KH và CN Quân sự, số Đặc san CNTT, 04 – 2019, ISSN: 1859 – 1043.

ABSTRACT

A NEW DIGITAL SIGNATURE SCHEME BASED ON THE DIFFICULTY OF THE DISCRETE LOGARIT COMBINING FINDING ROOT PROBLEM ON Z_P

The paper proposes to build a digital signature schema based on the difficulty of the discrete logarithm combining finding the root problem on Zp. This problem is a new difficult type of problems class without a mathematical solution. Building a digital signature scheme based on the difficulty of the discrete logarithm combining finding root problem allows improving the security of the algorithm. In addition, the signature schema construction method here can be applied to develop a new digital signature algorithm layer that is suitable for applications that require high levels of security in practice.

Keywords: Digital signature; Digital signature algorithm; Digital Signature Schema; Discrete Logarithm Problem; Finding Root Problem.

Nhận bài ngày 07 tháng 11 năm 2019
Hoàn thiện ngày 08 tháng 12 năm 2019
Chấp nhận đăng ngày 10 tháng 4 năm 2020

Địa chỉ: [1]Khoa CNTT, Cao đẳng KT-KT TPHCM;
[2]Khoa CNTT, Học viện KTQS.
*Email: thuyphulam2013@gmail.com.